Defense Horizons
Number 61
A publication of the
Center for Technology and National Security Policy
National Defense University
JANUARY 2008

Cyber Influence and International Security

by Franklin D. Kramer and Larry Wentz

Overview

Cyber influence is an ongoing source of power in the international security arena. Although the United States has an enormous cyber information capacity, its cyber influence is not proportional to that capacity. Impediments to American cyber influence include the vastness and complexity of the international information environment, multiplicity of cultures and differing audiences to which communications must be addressed, extensiveness and significance of contending or alternative messages, and complexity and importance of using appropriate influential messengers and message mechanisms.

Enhancing the influence of the United States in cyberspace will require a multifaceted strategy that differentiates the circumstances of the messages, key places of delivery, and sophistication with which messages are created and delivered, with particular focus on channels and messengers.

To improve in these areas, the United States must focus on actions that include discerning the nature of the audiences, societies, and cultures into which messages will be delivered; increasing the number of experts in geographic and cultural arenas, particularly in languages; augmenting resources for overall strategic communications and cyber influence efforts; encouraging long-term communications and cyber influence efforts along with short-term responses; and understanding that successful strategic communications and cyber influence operations cannot be achieved by the United States acting on its own; allies and partners are needed both to shape our messages and to support theirs.

The United States is an information superpower, estimated to produce annually about 40 percent of the world's new, stored information and a similar share of telecommunications.[1] U.S. dominance in information production might be expected to create commensurate influence, yet numerous opinion surveys show that approval of the United States is declining almost everywhere, as is American influence. In 2006, the Pew Global Attitudes Project found that "America's global image has again slipped" and that in only 4 of 14 countries surveyed did the United States have at least a 50 percent favorable rating as compared to 7 of 10 in 1999–2000.[2] A British Broadcasting Corporation (BBC) poll of some 26,000 people in 24 countries (including the United States) published in 2007 likewise confirmed that the "global perception of the U.S. continues to decline," with the populace of only 3 of the 24 countries surveyed saying the United States had a mainly positive impact on world affairs.[3] The mismatch between U.S. information capabilities and the actuality of U.S. influence is obvious.

This essay analyzes the factors that affect the generation of influence through cyber capabilities in the international security arena. For the United States to be more effective, a three-part cyber strategy must be developed that combines:

- psychological and marketing expertise in the application of the principles of influence
- domain expertise in the geographic, cultural, linguistic, and other arenas where the principles are to be applied
- technical and management expertise in the use of cyber capabilities and tactics.

Even with such capacities, however, U.S. cyber influence will be affected by numerous factors, including the nature of the

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JAN 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyber Influence and International Security (Defense Horizons, January 2008, Number 61)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Center for Technology and National Security Policy,300 5th Avenue, Fort Lesley J. McNair,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**12**	

information environment, the multiplicity of entities undertaking communications, the actions and policies of the relevant parties (including competing communications strategies of our adversaries), and the impact of culture, belief, and emotion.

Cyberspace Considerations

Cyberspace is "an operational domain characterized by the use of electronics and the electromagnetic spectrum to create, store, modify, and exchange information via networked information systems and associated physical infrastructures."[4] In cyberspace, information communications technologies are used to create and transmit information and thereby generate influence. The capacities of the different technologies overlap, especially as technological convergence continues through ever-greater reliance on digitization, computers, and the Internet. A look at the technologies reveals both their overlapping natures and their particular virtues.

Classic telecommunications were built on voice-grade, circuit-switched "plain old telephone service," which was oriented to end-to-end connection. Many of these features are now found in or transmitted by wireless platforms and capabilities, such as cell phones, WiFi and WiMax, faxes, smart phones (such as Blackberry and Treo), text messaging, and voice-over-Internet protocol. The dominant feature of the phone is speed of communication and, in its newer versions, a close approximation to "anywhere/anytime" contact.

Radio and television are top-down, one-way, broadcast communicators, divided among local, regional, or national systems and increasingly available on a continuous, often global basis through the use of satellite, cable, and streaming audio and video via the Internet. The dominant feature of radio and television is the capability to reach broadly over an area and, accordingly, provide information simultaneously to a very large audience.[5]

The Internet can be a one- or two-way (or more) channel that can have targeted or broad reach. The Internet can create focused groups, establish social networks, engage large populations, and allow for organization across borders. It tends to be a bottom-up, interactive, and instantaneous means of communicating. Its characteristics include "viral distribution" (the quick movement from one or a core to many through the capacity of message recipients to become message distributors), a capacity to search for and provide useful information for action and/or education, and an ability to create influence through the communications empowerment of individuals or groups.

Telecommunications, radio and television, and the Internet have all been enhanced by digitization and the creation of capacities for multiple sources of information—no longer limited to professionals—from cameras, camcorders, iPods, compact discs, digital video discs, and video and audio tapes. User-generated content—and a sort of collective intelligence—has become one of the dynamic and influential aspects of cyberspace via capabilities such as blogs and Wiki sites.[6]

In sum, the ability to use cyber capabilities to communicate in the modern world is substantial and increasing, but communication does not necessarily translate into influence.

From Communication to Influence

Translating communication into influence, particularly in the international arena, requires a full understanding of the factors that bear on the reception and interpretation of the message.

Complex Environment

The international information environment is vast and complex. Multiple messages are being sent and received by multiple entities, simultaneously and generally in an uncoordinated fashion. Even apart from the Internet, in the United States alone, each day there are more than 12 billion display and 184 billion classified advertising messages from newspapers; 6 billion messages from magazines; 2.6 million commercial (radio) messages; 330,000 television commercials; and 40 million direct-mail pieces.[7]

the ability to use cyber capabilities to communicate in the modern world is substantial and increasing, but communication does not necessarily translate into influence

Worldwide, in 2002, 18 exabytes (10^{18} bytes) of new information were produced through electronic channels (telephone, radio, television, Internet)[8] and 5 exabytes of new information were produced by print, film, magnetic, and optical storage media.[9] This translates to 800 megabytes of recorded information produced globally per person in 2002.[10] Worldwide, an estimated 25 billion emails per day were sent in 2006—not including spam messages, which account for 60 percent of all email.[11]

Of course, bytes are not the only or best way to measure the information flow. Video generates more bytes than text; all of Wikipedia will fit on a 100-gigabyte hard drive, which would store less than one day's worth of one channel of broadcast-quality TV programming. Another indicator of information flow is the more

Franklin D. Kramer is a Distinguished Research Fellow in the Center for Technology and National Security Policy (CTNSP) at the National Defense University (NDU). Larry Wentz is a Senior Research Fellow in CTNSP at NDU.

than 1.2 billion landline telephones and 2.1 billion cell phones that are in use worldwide.[12] Over 1 billion people (18.9 percent of the world's population) use the Internet.[13] From 2000 to 2007, Internet use jumped 244.7 percent globally, with the greatest percentage increases seen in Africa (874.6 percent) and the Middle East (920.2 percent).[14] More than 50 million blogs are maintained worldwide, a number that has doubled every 6 months for the past 3 years.[15]

As the foregoing suggests, the world is awash in information and means of communication, and the market for attention is highly complicated and competitive. The actors are diverse, ranging from individuals to private entities of all types to governments to supranational entities. The topics include economic, social, governmental, and all forms of human intercourse. Information overload and "noise" are serious problems that contribute to the masking of messages.

Information is continually circulating. Multiple perspectives are regularly presented, and access can be limited in certain areas by, for example, government action. In such an arena, even so substantial an entity as the U.S. Government is only one player. The information environment is not one in which "information dominance" or "information superiority"—in the sense of overwhelming the other players—is likely to be achieved.[16] "Information effectiveness," on the other hand, is achievable.

effective communication in the international arena is more difficult than communication in a familiar culture

Target-side Analysis

Communication influence is, of course, intended to affect a target or targets, whether one person or many, similar or divergent. But creating that influence requires much more than aiming communication at targets. Some key factors are considered below.

First, and most importantly, "Communication cannot be conceptualized as *transmission*. . . . The sense people make of . . . messages is never limited to what sources intend and is always enriched by the realities people bring to bear."[17] So, instead of a target or an audience, the other party should be considered an active participant. Hence, understanding the target participants is critical to creating the influence the communicator seeks to achieve.

Effective communication in the international arena is more difficult than communication in a familiar culture. Understanding values and belief structures, truly comprehending the language, and being knowledgeable about the information culture are key factors. One has a good feel for one's own culture, but it takes work to achieve a similar feel for another culture. For example, is the culture one where focus on the individual is the best approach, or is the group or the family more of the key influence mechanism? What is the power of the rumor mill and informal networking? What perceptions and biases should be anticipated? All these and many other cultural factors affect the influence of an international message.

Even though culture is a good starting point in thinking about how to create influence, culture is not everything. Interest issues—the political, social, and economic imperatives—also will have huge impact. So, too, will the role of the sources of influence in the society, including key individuals, trusted advisors, and influence networks.[18] The mindset and behavior of such individuals and networks will have significant impact on the interpretation of the message and, hence, on its influence.

In short, the communicator's problem is how to address simultaneously multiple communication partners. This problem is familiar in the context of U.S. political campaigns, where the communicators must reach the political base, the swing vote/neutrals, and the opposition, as well as pundits all at the same time. This problem is heightened in an international context. In the targeted nation or nations, there will be government officials, other key leaders, both political and private (for example, business and nongovernmental groups), and the population at large, which likely will be divided along racial, cultural, religious, and other lines. In addition, for many international messages, and certainly for the most important, other nations will be interested. That "group," of course, is also likely to be highly divergent, including friends and potential allies, neutrals, and potential or actual enemies. Moreover, the message we deliver to others also will be delivered to ourselves—to the affected portion of the government, the Congress, and the population at large.

Finally, whether the target partners are influenced by the message will be significantly affected by the fact that "research has shown that people inform themselves primarily at moments of need."[19] This has been found to be true in the context of American commercial and domestic political messaging campaigns. The issue of need requires evaluation in the context of an international geopolitical influence effort. Determining the need for information—and therefore the basis for influence—in a different society brings the communicator back to the importance of understanding that society, culture, interests, and entities.

Message Delivery

Understanding the target participants is only part of the communicator's challenge. A second key aspect is the delivery side of messaging: How are the contents of the message chosen? How are the delivery means chosen? How are the messengers chosen?

With respect to content, the most important understanding the communicator must achieve is that what he says is only part of the content. Already noted is the fact that the recipient will participate in shaping the message. Also of crucial importance,

however, is what might be called the "message-facts relationship." In speaking of the importance of information as a part of counterinsurgency warfare, David Galula, in his classic book on the subject, points out that "facts speak louder than words"; "[the counterinsurgent] is judged on what he does, not on what he says"; and "nothing could be worse than promising reforms and being unwilling or unable to implement them."[20]

Counterinsurgency is far from the only circumstance in which international messaging will be undertaken. The point, however, is universal: words can only go so far in the face of real-world evidence that undercuts them or is otherwise more influential.

One important aspect of which the communicator must be aware is the nonverbal message, which often is more influential than the verbal message. As an illustration, Colonel Ralph Hallenback, USA (Ret.), who operated in Iraq as a Coalition Provisional Authority (CPA) civilian, observed, "There has been much subsequent handwringing about CPA's lack of strategic communication with the Iraqi people. [But] a lot of people had no electricity but could look across the river and see the CPA all lit up at night. And that was the way we really communicated."[21] If the nonverbal message is not considered, unintended consequences may overwhelm the intended impact of the message.

Assuming that the message content will not be overwhelmed by the message context, the message must still be chosen to have the desired effect, given the nature of the target audience and the environment. Messages can be delivered directly or indirectly, and sometimes an indirect message may be more effective than a direct one. What might be considered a logical argument may have limited impact because the target participants have strongly held positions for cultural, emotional, or psychological reasons. For example, a campaign for the rule of law may be seen as undercutting the position of elders in a tribal society.

Few new messages have immediate impact, and the role of repetition must be considered—as must the role of timing and whether the message will fill an information need. Direct, hard-hitting confrontational messages also may be appropriate, depending on the results sought. But some messages will not work at all in some environments, although the desired effects may be achievable with a different message.

Different means of delivering messages will achieve different results. Cell phones were the great factor in Ukraine's Orange Revolution. User-generated content such as blogs and digital pictures have had great impact, most notoriously in the Abu Ghraib scandal. Television has had a decided impact on the world's view of the ongoing conflict in Iraq. Such cyber mechanisms, of course, can be complemented or outrun by simple word of mouth—rumor probably is the greatest factor in the views held by many in the Arab world as to who was responsible for the 9/11 attacks. For example, there is continued doubt in the Arab community that Muslims were involved, even after the release of the video in which Osama bin Laden takes credit for the attacks. The effective communicator will analyze the full spectrum of potential message arenas from word-of-mouth discussions, print media, cell and telephone capacities, data networks, including portals and messaging, and radio, television, and movies—all of which are complementary, and many of which are converging because of technological advances.

Different delivery means also may imply different messengers, and the choice of messenger is surely important.[22] A messenger may appeal to an audience for many reasons ranging from trust and respect to common interest to celebrity "buzz" to fear. The importance of the culturally attuned messenger is implicit in another point made by Galula, who stresses the importance of finding and organizing the "favorable minority."[23] In his analysis, that minority, working with the outside intervening power, has an important capacity to help resolve the insurgency issue. The reasons, of course, include the minority's understanding of the context for the insurgency and the ability to involve the rest of the country in its resolution. The lesson for the international communicator, more generally, is that communications undertaken with the help of knowledgeable, favorable, local messengers will have a greater chance of success,[24] both because third-party communications are often more effective than those of intervening outsiders, and because the knowledgeable local can help make outsiders more effective.

the effective communicator will analyze the full spectrum of potential message arenas—all of which are complementary, and many of which are converging because of technology advances

U.S. Cyber Capacities

The U.S. Government uses a variety of mechanisms to create influence in international cyberspace. For example, public affairs offices at the White House, the Department of State (DOS), the Agency for International Development (USAID), and the Department of Defense (DOD) all use television and radio appearances and maintain Web sites to deliver messages. The information is immediately available worldwide, generally circulated without charge by private media, and increasingly available for review on the Internet. The government's public affairs capacity is enhanced by numerous additional offices and multiple sites. Every Embassy has a public affairs activity, as do numerous DOD commands, and there are many Internet capabilities.

In addition to public affairs, the United States undertakes formal public diplomacy led by the Undersecretary of State for Public Diplomacy. The Public Diplomacy office emails fact sheets, news, event announcements, and electronic journals, and DOS experts are even made available electronically. Embassies also use cyber means, and Embassy Web sites present substantive material.

A third area of U.S. cyber capability is the Broadcasting Board of Governors (BBG).[25] Since October 1, 1999, the BBG has been the "independent federal agency responsible for all U.S. government and government sponsored, non-military, international broadcasting."[26] According to the BBG:

> every week, more than 100 million listeners, viewers, and internet users around the world turn-on, tune-in, and log-on to U.S. international broadcasting programs. . . . [D]ay-to-day broadcasting activities are carried out by individual BBG international broadcasters: the Voice of America (VOA), Alhurra [television], Radio Sawa, Radio Farda, Radio Free Europe/Radio Liberty (RFE/RL), Radio Free Asia (RFA), and Radio and TV Martí, with the assistance of the International Broadcasting Bureau (IBB).[27]

A fourth use of cyber capabilities by the U.S. Government is what DOD calls *information operations*, which include "electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities."[28] A key function of information operations is "influencing the way people receive, process, interpret, and use data, information, and knowledge."[29]

DOD also makes good use of cyber capabilities to create close partnerships with other countries as part of an overall information campaign. The Partnership for Peace Information Management System was established by DOD in 1996 to support the North Atlantic Treaty Organization's (NATO's) Partnership for Peace members and still seeks to "facilitate collaboration and strengthen relationships in the Euro-Atlantic and Partnership for Peace community."[30]

The Asia-Pacific Area Network was created in 1998. Hosted by U.S. Pacific Command, it is a "World Wide Web portal offering information resources and a collaborative planning environment as a means to greater defense interaction, confidence-building, and enhanced security cooperation in the Asia-Pacific Region."[31] DOD also uses its cyber capacity to plan, support, and conduct exercises on line to work with and influence others.[32]

to provide the right information at the right time and place to help achieve the desired effect, the government needs a comprehensive strategy and plan to focus on the target audience

As the foregoing suggests, the U.S. Government makes extensive use of cyber capacities, particularly the Internet. At State, for example, the USInfo site presents a large amount of information on a daily basis, not only in English, but also in Spanish, French, Russian, Chinese, Arabic, and Persian. State also runs ejournalUSA, which has articles in five thematic areas—Economic Perspectives, Global Issues, Issues of Democracy, Society and Values, and Foreign Policy Agenda—and is available in the same seven languages, plus Portuguese. DOD sponsors a number of information and online news Web sites. Some sites, such as ones maintained by U.S. Central Command, produce information relevant to some of the most difficult issues, particularly the war in Iraq. Others, such as the Southeastern European Times (published in nine languages) and Magharebia (published in three languages) provide "regional news," and "in-depth analysis" for their respective areas.[33] DOD networks also add to the government cyber use.

Creating a more effective U.S. Government use of cyberspace will involve more than simply getting more information online. To provide the right information at the right time and place to help achieve the desired effect, the government needs a comprehensive strategy and plan to focus on the target audience, including the audience's information culture and needs.

Issues for Cyber Effectiveness

As a general proposition, U.S. Government cyber communications focus on a "mass messaging" approach, seeking to enhance and increase information flow. Mass messages have an important function. It is a very big world, and the government has interests all around it. Simple practicality calls for the use of mass messages.

The downside of mass messages is that they are in transmission mode. As previously discussed, however, virtually no communication is received without the audience "being involved in creating meanings." Moreover, the meanings created will importantly reflect the target's culture. Thus, the issue that arises for the United States is what is often described as *segmentation*, dividing the mass audience to focus on specific receiver needs. Creating segmentation in a real world of multiple, overlapping audiences is a difficult, though not impossible, proposition.

It is not likely that the government will abandon the mass messaging approach. The White House Web site, the daily DOS Washington briefing, and numerous similar activities will continue. Segmentation, and a focus on the culture of less than an "all-world" mass audience, will need to be done by different message channels.

One obvious way to segment messages would be through the Embassy posts. There, however, the Government Accountability Office (GAO) has found government performance deficient, stating that posts did a "poor job of answering [the] basic question of whether to direct . . . communications efforts at a mass audience or opinion leaders."[34]

A second problem for creating effective messages arises from what can be called the "problem of multiplicity," almost always an issue for U.S. Government strategic messaging. For any communicator working on behalf of the government, it is important to recognize that the United States has multiple goals and operates in a very complex world. The profusion of messages that the government generates reduces its capacity to have a single, focused message on any particular topic.

A multiplicity of message follows from a multiplicity of policy, and a multiplicity of policy means that, sometimes, policies must be prioritized and even apparently inconsistent policies must be followed. Multiple policy objectives can create difficulties for consistent messaging. To take two obvious examples, the United States seeks good relations with both Japan and China. Because these two countries sometimes are at odds, positive messages to one can be seen as negative messages to the other. A similar messaging dilemma has occurred in the context of the Middle East peace process.

As noted earlier, it may be possible to help resolve the problem of multiplicity of messages by focusing on a regional or country basis. As a real-world matter, however, the GAO found that U.S. Embassies "did not have a core message or theme to direct their communications efforts." In fact, of the posts reviewed by GAO, none had a detailed communications plan.[35] This absence of thematic messaging is evident in the headline links of Web pages of American Embassies. The entries are perfectly reasonable topics for a Web page, but the pages lack thematic consistency and the pages simultaneously present very different kinds of messages. Part of the reason is that the Embassies are undertaking both long- and short-term messaging. Long-term efforts seek to build credibility and trust sufficient to sustain dialogue even amidst policy disputes. The focus is values-driven, and the expectation is that objective presentation of information will ultimately put the United States in a favorable light. This can be a reasonable function for mass messaging approaches. By contrast, short-term messaging is advocacy- and event-driven and seeks to build support for discrete U.S. policies. It is very unlikely, given the various audiences, values, interests, and actions relevant to a policy, that mass messaging will regularly produce short-term effects. A more tailored approach will be important.

public affairs messaging, particularly from the United States, is not a place where tailoring for a non-U.S. audience is easily undertaken

Evaluating U.S. Cyber Influence Effectiveness

U.S. status as an information superpower has not translated to international influence. Both the Pew poll published in mid-2006 and the BBC poll published in January 2007 underscore the declining international perception of the United States. The United States currently has this low standing despite a variety of efforts to improve its standing and regular use of the Internet and other communications means to make its points.

The problems associated with mass messaging, multiplicity of messages, and lack of core themes were discussed above. Other impediments to influence were addressed 60 years ago in the seminal research article, "Some Reasons Why Information Campaigns Fail."[36] To understand better how to "promote the free flow of ideas by word and image" on a worldwide basis, the authors focused on the "psychological barriers to the free flow of ideas." Based on the research, they reached some important conclusions.

First, there "exists a hard core of chronic 'know-nothings'"—persons who have little information about events. The study points out that "there is something about the uninformed which makes them harder to reach, no matter the level or nature of information."

Second, "interested people acquire the most information." Noting that "motivation" to acquire information is key, the study also recognizes that large groups in a population will have little or no interest and "such groups constitute a special problem which cannot be solved simply by 'increasing the flow of information.'"

Third, the study found that "people seek information congenial to prior attitudes."[37] They also "avoid exposure to information which is not congenial."[38] The study's important conclusion is that "[m]erely, 'increasing the flow' is not enough, if the information continues to 'flow' in the direction of those already on your side."

Fourth, "people interpret the same information differently. . . . It is . . . false to assume that exposure, once achieved, results in a uniform interpretation and retention of the material. . . . [I]t has been consistently demonstrated that a person's perception and memory of materials shown to him are often distorted by his wishes, motives, and attitudes. . . . Exposure in itself is not always sufficient. People will interpret the information in different ways, according to their prior attitudes."

Fifth, and perhaps most importantly, "information does not necessarily change attitudes":

> The principle behind all information campaigns is that disseminated information will alter attitudes or conduct. There is abundant evidence in all fields, of course, that informed

> people actually do react differently to a problem than uninformed people do. But it is naïve to suppose that information always affects attitudes, or that it affects all attitudes equally. The general principle needs serious qualification. There is evidence . . . that individuals, once they are exposed to information, change their views *differentially*, each in the light of his own *prior* attitude.

Sixth, and in light of the foregoing, the authors reached the conclusion that the "above findings indicate clearly that those responsible for information campaigns cannot rely simply on 'increasing the flow' to spread information effectively."

The implications of these conclusions for the effectiveness of U.S. cyber influence are substantial. Information will tend to be accepted and understood in light of prior attitudes; those already supportive of U.S. positions will be most likely to accept information from the United States. Some groups simply will not accept information. If it is important to change their attitudes, more than a direct information approach will be necessary. Determining how to change the positions of those in opposition is more difficult, since these people may interpret the information provided quite differently than intended, according to their prior attitudes.

understanding the psychological and marketing issues inherent in influence campaigns is crucial

Enhancing U.S. Cyber Influence

Enhancing the influence of the United States in cyberspace will require a multifaceted strategy that differentiates the circumstances of the message, the key places of delivery, and the sophistication with which the message is created and delivered, with particular focus on channels and messengers.

A useful starting point is to distinguish among three different analytic circumstances. The first might be called the *general condition* under which the United States will have a great many messages on a great many topics that it is regularly delivering. Those messages are normally delivered by the public affairs functions of the government, as exemplified by the DOS spokesperson's briefings. Even though the messages are focused on international topics, quite often the intended first recipient of the message is the American public. For example, at a DOS briefing, numerous U.S. media entities will be present, and they will pass on the message to the American public. Of course, international media are also present, and the messages also will be presented internationally—but the message will always be intended to make sense to the American public.

The key conclusion from this analysis is that public affairs messaging, particularly from the United States, is not a place where tailoring for a non-U.S. audience is easily undertaken. Messages delivered in American English will have a "made in America" tenor. This is not a "bad" result; in fact, it is a "good" result because the American people should have a full understanding of government policy. But it does mean that public affairs undertaken from the United States cannot easily take account of the multiple factors that make international messaging difficult.

Often, in discussions of the effectiveness of U.S. international messaging, there are suggestions that one strategic message should be undertaken top to bottom—so to speak, from the President to the junior Foreign Service Officer and the Army private. But Presidential addresses on international matters are almost always, first and foremost, statements to the American people. Such statements obviously will be the substantive heart of the international message. But they will not be tailored to the international audience. For Presidential addresses and for building on public affairs messages in general, additional international messaging will be necessary for, among other things, reaching the uninformed, those who do not already agree with the substance of the message, and those whose prior attitudes will affect how they understand the message; being part of an influence effort to affect the views of those who will not change their minds simply because of exposure; and generating effective communication with key leaders and organizations.

The second circumstance is what might be called the *focused, non-wartime problem.* Some examples of topics are global warming, responding to radical militant Islam, and promoting free trade in Asia. These problems are focused in that they need to be considered. They are non-wartime in the sense that the violent use of force is not ongoing (or at least not as a major factor). The assumption is that, in a war, the impact of combat generally will overwhelm the use of words.

Effective cyber influence in a focused, non-wartime problem requires taking account of numerous considerations and constraints. The complexity of the environment and the numerous messages can be somewhat simplified because of the focus on particular messages. A good first step would be for the United States to create an "international map" of individuals and entities important to influence. Not all the world is critical in the same way on every issue. Not only will the messengers be different, but so will the opposition affected by prior attitudes and/or ignorance whose concurrence with U.S. views will be necessary or valuable.

With this map in hand, a cyber influence campaign can be planned. The next step will be to understand the culture in which influence is sought—how will those who get messages view and respond to them? In thinking through message presentation, some

questions can be key (and the particular culture may make others important). The following are examples:

- What is the desired effect?
- Should focus be on the individual, or is the group (for example, the family) more the key influence mechanism?
- Will negative messaging work?
- What is the role of religion, and how does that affect messaging?
- What is the meaning of success (for example, is it better for an individual to stand out, or to support another)?
- How do you pretest messages and determine what has been successful?
- Who is the correct messenger? Would a third party be more effective?

Likewise, the interests and nature of key entities must be considered. How does the U.S. message, if adopted, affect the political, social, and economic imperatives of the target audience? Who are the important sources of influence in the society, including key individuals and trusted advisors and influence networks? Galula's point about building on the favorable minority surely must be considered.

None of the foregoing can be undertaken effectively unless experts in the geographic and cultural areas where influence is sought (including some experts with a deep understanding of the language) are heavily involved in the development of the message. Those experts can help build the map and describe the culture and relevant interests, as well as the individuals and entities of influence.

Such domain expertise is necessary but not sufficient for effective cyber influence. Understanding the psychological and marketing issues inherent in influence campaigns is also crucial. The insights of "Some Reasons Why Information Campaigns Fail" are good examples of the psychology behind an influence campaign. Marketing expertise likewise should be understood. These matters, however, raise the crucial factor of intercultural expertise. What is true in the United States in terms of psychology and marketing may not be true in another culture. It is the rare person who will combine cultural and geopolitical expertise with psychological and marketing expertise. An interdisciplinary team is needed.

The interdisciplinary team also will need a member with a third expertise, namely, in the use of cyber techniques—how to make effective use of radio and TV, what can be accomplished by cell phone messaging, how to use the Internet. In the international context, this type of expertise will necessarily have to be combined with cultural, language, and psychological expertise to be effective. As the team generates its approach, it also will need to consider how cyber and noncyber activities interact.

A final point on the focused, non-wartime message is that the concept of focus deserves much more attention. If everything is equally important, it is very hard to give focus. But, as the discussion of the Embassy Web sites suggests, the United States has made few attempts to focus its messages in the international arena. In fact, that is the point of the GAO study, which stated that U.S. Embassies "did not have a core message or theme to direct their communications efforts." Of the posts reviewed, none had a detailed communications plan.

The DOS Office of Public Diplomacy has recognized the importance of focus and has identified three key themes: support the President's Freedom Agenda with a positive image of hope, isolate and marginalize extremists, and promote understanding regarding shared values and common interests between Americans and peoples of different countries, cultures, and faiths.[39] If these are to be the key themes, it will be important not only for a Washington office to assert them, but also for posts abroad to do so. It is also important to ask *when and where the themes are relevant*. In some situations, the themes, though most important to Washington and presumably to a number of other countries, may not be the best messages for some target countries. The need to decide the key themes, and when and where to implement them, leads to a requirement for a strategic plan. As the GAO study indicates, such plans are required. For the most part, they are not undertaken. That is a crucial failing—and until it is corrected, it is unlikely that U.S. influence campaigns, including cyber influence campaigns, will become more effective.

the three types of expertise—geographic and cultural, psychological and marketing, and cyber technical—necessary for effective cyber communications need to be organized and coordinated with the military

The last analytic circumstance to be considered is cyber influence in the *wartime situation*, that is, where the use of violence is a major consideration. The ongoing situations in Iraq and Afghanistan are examples, as is the introduction of the military into so-called stability operations (including counterinsurgency, peace enforcement, and peacekeeping).

Military involvement does not mean that influence is not a critical factor. Clausewitz's observation that war is a continuation of

politics by other means emphasized the importance of the intended political outcome over the particular means employed to achieve it. In a wartime situation, a dominant factor in generating influence will be the use or threat of violence. The impact of the normal influence channels, including cyber influence, will be relatively less because the impact of violence will be so great. However, the generation of cyber influence is still applicable, though more complex. A domain expertise in three arenas—geographic and cultural, psychological and marketing, and cyber technical, including planners and implementers—is still needed. But in addition, the interface with the military must be considered. In this regard, several points deserve consideration.

while neither a cyber nor any other influence campaign can provide magical results, an effective use of cyber capabilities can do much

First, the public affairs efforts of the U.S. Government are going to continue in a wartime situation. Those efforts, first and foremost, will be directed toward providing information to the American public. There is no point in asking for such messages to be focused on the theater of operations because, for the most part, that will not happen.[40] What can happen, however, is for the public affairs personnel to be highly aware of the theater requirements and, at a minimum, communicate and, when possible, coordinate messages. As an example, in the Kosovo campaign undertaken under NATO auspices, both interagency and international communications groups undertook such efforts.

Second, the three types of expertise—geographic and cultural, psychological and marketing, and cyber technical—necessary for effective cyber communications need to be organized and coordinated with the military. To accomplish this, two fundamental shortcomings of the current system must be overcome.

The first shortcoming is that the necessary expertise does not exist in sufficient capacity or at high enough levels in the government. A much greater capacity in both DOS and DOD is necessary. Achieving that level of capacity and expertise can involve a combination of permanent personnel, reserve personnel, and contractors—but the first step is recognizing that we are not even remotely close to the level of expertise we need.

The second shortcoming is that we do not make good use of the capacities we do have. In a wartime situation, the military undertakes to do the best it can in terms of influence operations. A very impressive example is set forth by Colonel Ralph Baker, USA, in his discussion of how he used information operations as one of his "vital tools" to "favorably influence the perceptions of the Iraqi population" in his area of operations.[41] But Baker's story is one of improvisation, not of a strategic campaign effort. As he says, the "traditional tools in my military kit bag were insufficient to successfully compete" in the influence environment.

Unfortunately, it is not only the lone brigade commander who lacks the tools. DOS generally is not an effective player in influence operations in the theater situation, and DOD does not have adequate theater capacity—or, as Baker makes clear, tactical capability.[42] Contractors have been used, but the results on the whole have not been satisfactory. For example, it is generally agreed that, after the end of major combat operations in Iraq in 2003, it took far too long to generate a U.S.-supported television capability. Achieving better results will require a more coordinated, effective, interagency approach. Up to now, the United States has not been able to accomplish that, even though it is engaged in several wartime situations.

The final point is that even though violence or the threat of violence has a major influence impact, there is also an extremely important role in influencing target populations as to what the impact of violence should mean to them. As an example, in the Israeli-Hizballah conflict in 2006, both sides mounted intensive influence campaigns designed to show they were winning and that they deserved the support of several audiences—their own people, allies, potential intervening states, sympathetic populations and countries, and the world at large. Whenever war will not be fought to a conclusion of unconditional surrender or destruction (and perhaps even then), the method and consequences of conflict termination will be affected by more than one combatant. Hence, influencing the perceptions and consequent actions of relevant target audiences is of greatest importance to the combatants.

Conclusion

Cyber influence is an ongoing source of power in the international security arena. Although the United States has an enormous cyber information capacity, it has less cyber influence than might be desirable. While neither a cyber nor any other influence campaign can provide magical results, an effective use of cyber capabilities can do much. A considered approach that recognizes the context in which cyber capabilities will be used; understands the principles of making influence campaigns effective; and provides personnel expertise in the technical management of cyber capabilities, in the domains—particularly cultural and geographic—where they will be applied, and in psychological and marketing expertise relevant to the use of cyber capabilities, should be an important component of international security activities for the United States.

In light of the foregoing, the following actions are offered for consideration as possible ways to help make U.S. cyber influence more effective in the international security arena.

First, and perhaps most importantly, greater focus must be placed on the nature of audiences and of the societies and cultures into which cyber-transmitted messages will be delivered. In the first instance, the intended recipients of messages need to be clear. For example, in the context of a counterterror effort, there likely will be a difference among messages to populations at large—those who do not support terrorists, those who are terrorist sympathizers, those who are active supporters of terrorists, and those who are terrorists. Moreover, those varying audiences might well be reached by different types of communications—for example, television for broader audiences and Web sites for potential terrorist recruits. In this context of differentiated messaging, a further important consideration needs to be an understanding of the types of persons who have influence with the message recipients and the types of contexts in which that influence will be most effective.

greater focus must be placed on the nature of audiences and of the societies and cultures into which cyber-transmitted messages will be delivered

Second, and implied by the first, it will be necessary to increase the number of experts in geographic and cultural arenas, including a greater expertise in languages. Such expertise can help build a societal/cultural map of influencers, key communications nodes, and cultural communications patterns to guide strategic communications and influence operations. Added to these cultural experts should be experts in psychology and marketing who can help generate messages and ensure that communications are effective. Finally, experts are needed in the use of television, radio, the Internet, and cell phones. In short, an interdisciplinary approach is required.

Third, leaders must realize that while there may be a consistent base message, that message will be presented in multiple theaters. These areas will differ significantly, and one should expect that, to be effective, messaging will likewise differ. To use an example, the society, culture, and influential persons in Indonesia are significantly different from those in Pakistan, and both are significantly different from those in Egypt. It is also worth noting that the Internet has created coherent, nongeographic communities. Numerous studies and reports document the Internet's effectiveness in transmitting messages that sympathize with, give support to, and recruit for terrorist efforts. The Internet must be a focused arena for strategic communications and influence operations.

Fourth, greater resources must be given to the overall strategic communications and influence efforts. For example, expanding the capacities of the Broadcasting Board of Governors, the Embassies, and other outlets of the State Department would be enormously valuable. As noted, the Internet is a key mechanism. DOS runs Web sites, but a broader and more multifaceted Internet strategy—both globally and regionally—would be highly desirable. The GAO has found that while Embassy posts are supposed to have a strategic communications plan, they are generally ineffective, with little focus and not enough resources.[43] Enhancing U.S. Government capabilities is a critical requirement.

Fifth, long-term communication efforts must be encouraged along with short-term responses. It is possible to change attitudes over time. As an example, consider the American attitude toward smoking, which has changed significantly over the last 30 years. In the battle of ideas, the U.S. Government is seeking a long-term change—and so there is a need to adopt long-term policies. As examples of useful approaches, the DOD Web sites, Southeast European Times, and Magharebia mentioned earlier provide news, analysis, and information that are productive, long-term approaches that will not affect attitudes immediately but can have significant consequences over time.

Sixth, the dictum "facts speak louder than words" must be fully appreciated. Some policies generate significant opposition, and strategic communications and influence operations are not panaceas that can overcome all real-world actions. In the earliest planning stages, the communications consequences of actions must be discussed. In conflicts, such as Iraq and Afghanistan, the impact of violent activities will very significantly change the views of the world—not only of those immediately impacted but of those who are indirectly affected and those to whom those impacts are communicated. Every battle commander in these irregular wars soon finds out that the communications battle is critical—because the center of gravity for success is the population. But all too often, our commanders have to learn this on the ground. Especially in this globalized world of instant communications, tactical actions can have strategic consequences. Cyberspace is a creative and cultural commons defined by information, perception, cognition, and belief, and it is becoming the preeminent domain of political victory or defeat. Increased support for training and resources for cyber-enabled communications will be critical elements of effective counterinsurgency and stability operations. As Galula argued, communication—to one's supporters,

Defense Horizons *is published by the Center for Technology and National Security Policy. CTNSP publications are available online at http://www.ndu.edu/ctnsp/publications.html.*

The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Department of Defense or any other department or agency of the Federal Government.

Center for Technology and National Security Policy

Hans Binnendijk
Director

to the population at large, and to the opposition—is of crucial importance. The government needs resources and training for our people on these issues, and these must be undertaken not only by DOD, but also in a joint DOD-State context.

Seventh, the U.S. Government should not expect to be successful at strategic communications and influence operations acting solely on its own. Rather, it should use an alliance and partnership approach, both to expand capacities and increase effectiveness. In the business world, it would be the rare American company that would seek to enter another country without the guidance and support of local business, whether as partners, joint ventures, or advisors—and often all three. In military and diplomatic arenas, our allies and partners are recognized as enormous sources of strength. In the strategic communications and influence operations arena, we need to develop those alliances and partnerships, both to shape our own messages and support theirs.

cyberspace is a creative and cultural commons defined by information, perception, cognition, and belief, and it is becoming the preeminent domain of political victory or defeat

Notes

[1] University of California Berkeley, *How Much Information? 2003*, Executive Summary, available at <http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/execsum.htm>.

[2] Pew Global Attitudes Project, available at <http://pewglobal.org/reports/display.php?ReportID=252>.

[3] BBC, World Service Poll, available at <http://news.bbc.co.uk/2/hi/americas/6288933.stm>.

[4] Daniel Kuehl, "Cyberspace—Cyberpower—Cyberstrategy: Their Influence on (Future) History," National Defense University Center for Technology and National Security Policy (forthcoming).

[5] The proliferation of channels in some areas has allowed for greater market segmentation and somewhat less "mass" mass marketing.

[6] Wiki is server software that allows users to freely create and edit Web page content using any Web browser. Wiki supports hyperlinks and has simple text syntax for creating new pages and crosslinks between internal pages on the fly.

[7] Michael Pfau and Roxanne Parrott, *Persuasive Communication Campaigns* (Boston: Allyn and Bacon, 1993).

[8] Two exabytes equals the total volume of information generated in 1999; 5 exabytes equals all words ever spoken by human beings. *How Much Information? 2003*, table 1.1.

[9] Ibid., Summary of Findings I.1.

[10] Ibid.: "It would take about 30 feet of books to store the equivalent of 800 MB of information on paper."

[11] Ferris Research, available at <http://www.ferris.com/research-library/industry-statistics>.

[12] *The World Fact Book* (Washington, DC: Central Intelligence Agency, 2007), available at <https://www.cia.gov/cia/publications/factbook/geos/xx.html>.

[13] Internet World Stats, accessed at <http://www.internetworldstats.com/stats.htm>.

[14] Ibid.

[15] Technorati, accessed at <http://www.sifry.com/alerts/archives/000436.html>.

[16] *Information superiority* is "the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." *DOD Dictionary of Military and Associated Terms*, April 12, 2001, as amended through April 14, 2006, available at <http://www.dtic.mil/doctrine/jel/doddict/data/i/02656.html>. See generally, Martin Libicki, "Information Dominance," *Strategic Forum* 132 (Washington, DC: National Defense University Press, November 1997), available at <http://www.ndu.edu/inss/strforum/SF132/forum132.html>.

[17] *Persuasive Communication Campaigns*, 53.

[18] See generally Malcolm Gladwell, *The Tipping Point: How Little Things Can Make a Big Difference* (Boston: Back Bay Books, 2002).

[19] *Persuasive Communication Campaigns*, 54.

[20] David Galula, *Counterinsurgency Warfare: Theory and Practice* (London: Praeger, 1964), 14, 104.

[21] Quoted in Thomas Ricks, *Fiasco: The American Military Adventure in Iraq* (New York: Penguin Press, 2006), 326.

[22] Malcolm Gladwell describes different types of influential messengers based on the category of what they are doing: *mavens*, who validate the message; *connectors*, who link different parties and groups; and *salesmen*, who are effective at marketing. All of these may play roles in the international influence arena.

[23] *Counterinsurgency Warfare*, 75–77.

[24] Gladwell, 219: "Simply by finding and reaching those few special people who hold so much social power, we can shape the course of social epidemics." Local assistance can help in both pretesting messages and assessing their impact.

[25] The BBG was created by the 1998 Foreign Affairs Reform and Restructuring Act (Public Law 105-277).

[26] BBG Online, available at <http://www.bbg.gov/bbg_aboutus.cfm>.

[27] Ibid.

[28] Joint Publication 3–13, *Information Operations* (Washington, DC: Office of the Joint Chiefs of Staff, February 13, 2006), GL–9.

[29] Ibid., I–9.

[30] Partnership for Peace Information Management System, available at <http://www.pims.org>.

[31] Asia-Pacific Area Network, available at <http://www1.apan-info.net/About/tabid/54/Default.aspx>.

[32] Ibid. The home page lists several exercises supported by the Asia-Pacific Area Network.

[33] Southeast European Times averages 5 million hits a month, with average visits exceeding 20 minutes. Charles F. Wald, "The Phase Zero Campaign," *Joint Force Quarterly* 43 (4th Quarter 2006), 72.

[34] Jesse T. Ford, Director, International Affairs and Trade, "U.S. Public Diplomacy, State Department Efforts to Engage Muslim Audiences Lack Certain Communication Elements and Face Significant Challenges," testimony before the Subcommittee on Science, the Departments of State, Justice, and Commerce, and Related Agencies, House Committee on Appropriations, GAO-06-707T (Washington, DC: U.S. Government Accountability Office, May 2006), 21; available at <http://www.gao.gov/new.items/d06535.pdf >.

[35] Ibid., 20, 21, 24, 26.

[36] Herbert H. Hyman and Paul B. Sheatsley, "Some Reasons Why Information Campaigns Fail," *The Public Opinion Quarterly* 11, no. 3 (Autumn 1947), 412–423.

[37] Ibid., 417.

[38] Ibid.

[39] Ford, 27.

[40] Public affairs activities at the local and regional level, for example, at Embassies, that can be focused on the theater of operations.

[41] Ralph Baker, "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations," *Military Review* (May-June 2006), 13.

[42] In a forthcoming companion piece to this article, Stuart Starr discusses how tactical influence operations might be improved.

[43] Ford, 20.

Other recent titles from
NDU Press

After the Surge: Next Steps in Iraq?
Judith S. Yaphe
(Strategic Forum No. 230, February 2008)

Organizing for National Security: Unification or Coordination?
James M. Keagle and Adrian R. Martin
(Center for Technology and National Security Policy, Defense Horizons 60, January 2008)

Strategic Fragility: Infrastructure Protection and National Security in the Information Age
Robert A. Miller and Irving Lachow
(Center for Technology and National Security Policy, Defense Horizons 59, January 2008)

The European Union: Measuring Counterterrorism Cooperation
David T. Armitage, Jr.
(Strategic Forum No. 229, November 2007)

Trans-American Security: What's Missing?
Luigi R. Einaudi
(Strategic Forum No. 228, September 2007)

The Country Team: Restructuring America's First Line of Engagement
Robert B. Oakley and Michael Casey, Jr.
(Strategic Forum No. 227, September 2007)

The Comprehensive Approach Initiative: Future Options for NATO
Friis Arne Petersen and Hans Binnendijk
(Center for Technology and National Security Policy, Defense Horizons 58, September 2007)

Privatizing While Transforming
Marion E. "Spike" Bowman
(Center for Technology and National Security Policy, Defense Horizons 57, July 2007)

China's ASAT Test: Motivations and Implications
Phillip C. Saunders and Charles D. Lutes
(INSS Special Report, June 2007)

Responding in the Homeland: A Snapshot of NATO's Readiness for CBRN Attacks
Michael Moodie and Robert E. Armstrong with Tyler Merkeley
(Center for Technology and National Security Policy, Defense Horizons 56, June 2007)

Counterintelligence and National Strategy
Michelle Van Cleave
(School for National Security Executive Education Report, April 2007)

Sino-Japanese Rivalry: Implications for U.S. Policy
(INSS Special Report, April 2007)

Preventing Balkan Conflict: The Role of Euroatlantic Institutions
Jeffrey Simon
(Strategic Forum No. 226, April 2007)

For on-line access to **NDU Press publications,** go to: **ndupress.ndu.edu**